Notice of Allowability	Application No.	Applicant(s)	
	10/813,920	TERVO ET AL.	
	Examiner	Art Unit	
	Andrew Wendell	2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/3/2006*.

2. ☒ The allowed claim(s) is/are *2-10,12,14,15,17,18,21 and 26-29*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Andrew Hyman on 10/10/2006 and 10/12/2006.

3. The application has been amended as follows:

In the Claims:

Claim 4, line 1, after "A method", insert -- for increasing security of a mobile terminal --;

Claim 4, line 12, at the beginning of the line, insert -- if the mobile terminal lacks the device management feature, --;

Claim 4, lines 14 and 15, delete "if the mobile terminal lacks the device management feature,"

Claim 26, line 1, after "Apparatus", insert -- for increasing security of a mobile terminal --;

Claim 26, line 11, at the beginning of the line, insert -- if the mobile terminal lacks the device management feature, --;

Claim 26, lines 13 and 14, delete "if the mobile terminal lacks the device management feature,"

Claim 28, line 1 after "Apparatus", insert -- for increasing security of a mobile terminal --;

Claim 28 lines 10, at the beginning of the line, insert – if the mobile terminal lacks the device management feature, --;

Claim 28 lines 11 and 12, delete "if the mobile terminal lacks the device management feature,".

Allowable Subject Matter

4. Claims 2-10, 12, 14-15, 17-18, 21, and 26-29 are allowable over the cited prior art.

5. The following is an examiner's statement of reasons for allowance: The prior art of record, Morriss et al. (US Pat Pub# 2004/0203601) in view of Kokubo (US Pat Pub# 2004/0224665) teaches regarding claim 4, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device teaches a transceiver for receiving a guard message 101 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal (Section 0011); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0011), a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0004), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0011), and employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging

(wireless messages, section 0054). Morriss et al. fails to teach destroying data and uploading the data.

Kokubo's mobile terminal apparatus teaches a transceiver for receiving a guard message 100 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal S601and S602 (Fig. 6); a communication locking mechanism S605 (Fig. 6), responsive to the authentication signal S602 (Fig. 6); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6); a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0046), and wherein the data securing mechanism is also for destroying S608 (Fig. 6) the at least part of the stored data is accomplished after uploading S606 (Fig. 6) the at least part of the stored data from the mobile terminal, and wherein the guard message employs synchronization markup language device management (e-mail, sections 0045-0046).

The prior art of record fails to teach a method for increasing security of a mobile terminal comprising inputting a personal identification code, at a location separate from a mobile terminal that has been lost, stolen, or misplaced, sending the personal identification code via a telephone connection to an automated or human attendant, receiving the personal identification code and using the personal identification code to determine from a database whether the mobile terminal has a device management

feature supporting synchronization markup language, composing a guard message that employs synchronization markup language if the mobile terminal has the device management feature, if the mobile terminal lacks the device management feature, composing the guard message so the guard message instead employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, sending the guard message from the attendant to the mobile terminal, authenticating the guard message at the mobile terminal, locking at least one communication capability of the mobile terminal, and securing at least some data that is stored in the mobile terminal.

Tett (US Pat# 5,604,788) teaches sending out a message according to customer coverage options 58 (Fig. 2), but Tett's invention is not related to securing a mobile terminal. Also, based on applicant's remarks submitted on 8/3/2006 further support the claim to be in allowance over prior art.

The prior art of record fails to teach the claimed subject matter as claimed and substantially connected in claims 2-10 and 12.

Regarding claim 26, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device teaches a transceiver for receiving a guard message 101 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal (Section 0011); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0011), a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile

terminal (Section 0004), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0011), and employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging (wireless messages, section 0054). Morriss et al. fails to teach destroying data and uploading the data.

Kokubo's mobile terminal apparatus teaches a transceiver for receiving a guard message 100 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal S601and S602 (Fig. 6); a communication locking mechanism S605 (Fig. 6), responsive to the authentication signal S602 (Fig. 6); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6); a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0046), and wherein the data securing mechanism is also for destroying S608 (Fig. 6) the at least part of the stored data is accomplished after uploading S606 (Fig. 6) the at least part of the stored data from the mobile terminal, and wherein the guard message employs synchronization markup language device management (e-mail, sections 0045-0046).

The prior art of record fails to teach apparatus for increasing security of a mobile terminal comprising a receiver device configured to receive a personal identification

code of a mobile terminal that has been lost, stolen, or misplaced; a database configured to reveal whether the mobile terminal corresponding to the personal identification code has a device management feature supporting synchronization markup language; and a messaging device configured to compose and send a guard message to the mobile terminal; wherein the messaging device is configured to employ a synchronization markup language if the mobile terminal has the device management feature, if the mobile terminal lacks the device management feature, wherein the messaging device instead employ a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, wherein the guard message contains instructions for the mobile terminal to lock at least one communication capability of the mobile terminal, and secure at least some data that is stored in the mobile terminal.

Tett (US Pat# 5,604,788) teaches sending out a message according to customer coverage options 58 (Fig. 2), but Tett's invention is not related to securing a mobile terminal. Also, based on applicant's remarks submitted on 8/3/2006 further support the claim to be in allowance over prior art.

The prior art of record fails to teach the claimed subject matter as claimed and substantially connected in claims 14-15, 17-18, 21, and 26.

Regarding claim 28, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device teaches a transceiver for receiving a guard message 101 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal (Section 0011); a communication locking mechanism,

responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0011), a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0004), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0011), and employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging (wireless messages, section 0054). Morriss et al. fails to teach destroying data and uploading the data.

Kokubo's mobile terminal apparatus teaches a transceiver for receiving a guard message 100 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal S601and S602 (Fig. 6); a communication locking mechanism S605 (Fig. 6), responsive to the authentication signal S602 (Fig. 6); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6); a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0046), and wherein the data securing mechanism is also for destroying S608 (Fig. 6) the at least part of the stored data is accomplished after uploading S606 (Fig. 6) the at least part of the stored data from the

mobile terminal, and wherein the guard message employs synchronization markup language device management (e-mail, sections 0045-0046).

The prior art of record fails to teach apparatus for increasing security of a mobile terminal comprising means for receiving a personal identification code of a mobile terminal that has been lost, stolen, or misplaced; means for revealing whether the mobile terminal corresponding to the personal identification code has a device management feature supporting synchronization markup language; and means for composing and sending a guard message to the mobile terminal; wherein the guard message employs a synchronization markup language if the mobile terminal has the device management feature, if the mobile terminal lacks the device management feature, wherein the guard message instead employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging, wherein the guard message contains instructions for the mobile terminal to lock at least one communication capability of the mobile terminal, and secure at least some data that is stored in the mobile terminal.

Tett (US Pat# 5,604,788) teaches sending out a message according to customer coverage options 58 (Fig. 2), but Tett's invention is not related to securing a mobile terminal. Also, based on applicant's remarks submitted on 8/3/2006 further support the claim to be in allowance over prior art.

The prior art of record fails to teach the claimed subject matter as claimed and substantially connected in claims 28 and 29.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew Wendell whose telephone number is 571-272-0557. The examiner can normally be reached on 7:30-5 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on 571-272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

10/16/06

QUOCHIEN B. VUONG
PRIMARY EXAMINER

Andrew Wendell
Examiner
Art Unit 2618